



Q131
#4/A
~~RECEIVED~~
OCT 26 2001
Technology Center 2100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

501.40397X00

Applicant(s): M. NISHIOKA, et al

Serial No.: 09/890,286

Filed: July 27, 2001

For: PUBLIC-KEY ENCRYPTION AND KEY-SHARING METHODS

Group: Not yet assigned

Examiner: Not yet assigned

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

October 24, 2001

Sir:

Prior to examination, please amend the above-identified application as follows.

IN THE CLAIMS

Please cancel claims 14-17 without prejudice or disclaimer of the subject matter thereof.

Please amend the claims as follows:

2. (Amended) A public-key encryption method for data transmitted between a sender who encrypts data to send with a public key and a receiver who decrypts the data encrypted and delivered to the receiver with a secret key corresponding to said public key, said public-key encryption method comprising:

(a) a key generation step which the receiver conducts by working the receiver-end device, according to a procedure comprising: